
Standards Management Process Working Group (SMP WG)

**Report to the
Standards Coordinating Committee
Chair and Membership**

11 August 2000

SMP Working Group Tasking

- **Background:** CFITS wished to evaluate revitalization of the SCC; review of draft mission & functions at May 00 SCC meeting generated comment on whether the SCC should continue as a sub-panel under the MCEB. SCC Vice-chair tasked the SMP WG to evaluate alternatives to the SCC current organizational structure and alignment under MCEB.
- **Issue:** Current DoD Information Technology (IT) standards management process, oversight and organizational structure appears inefficient for developing, coordinating, prescribing, and enforcing IT and NSS standards across all DoD in view of changes rendered by Clinger-Cohen Act.

SMP Working Group Tasking

- Review SCC's official and de jour functions, responsibilities, and scope of authority
- Review subordinate Standard Management Committee's (SMCs) functions and organization
- Review of current standards management process, lines of authority, oversight structure, reporting structure, and enforcement mechanisms for IT/NSS standards management in DoD to avoid redundant processes
- Conduct gap analysis and provide SCC members with alternatives for improvement and streamlining IT standards management in DoD

SMP Working Group Participants

Chair: Kris Strance -- OASD (C3I)/DCIO

- **CAPT Diana Turonis -- JFCOM(J6)**
- **Charles Schaffer -- Joint Staff (J6)**
- **Paul Fong -- Joint Staff (J6)**
- **Rex McKinnon -- AFCA/ITS**
- **Steve Klynsma -- USA/D2SC4**
- **Bonnie Smith -- DTRA**
- **Elaine Babcock -- CFITS**
- **MaryAnn Andersen -- CFITS**
- **Richard Walker -- CFITS**
- **Steven Thompson -- CFITS**
- **Glenn Plonk -- NSA**
- **Frank Hudson --AC2IRSC/C2PM**

SMP WG reviewed information/briefs on:

- **U.S. Military Communications-Electronics Board (MCEB)**
- **Global Information Grid/DoD Chief Information Officer's (CIO) Functions & Responsibilities**
- **DoD CIO Executive Board**
- **Architecture Coordination Council (ACC)**
- **Defense Standardization Program (DSP)**
- **DISA Center for Information Technology Standards (CFITS)**
- **Public Laws, Federal Regulations, and DoD Directives & Policies pertaining to IT Standards (NSS and ITS)**
- **Unified Command Plan '99/JFCOM Roles & Mission**

IT Standards Management Evolution

- **Nov 90** -- SECDEF assigns ASD (C3I) authority to establish and implement ADP standards for DoD
- **Dec 90** -- DEPSECDEF affirms that ASD (C3I) will integrate all DoD computing, telecommunications, and information management activities
- **Sept 91** -- ASD (C3I) assigns DISA Executive Agent responsibilities for coordinating and integrating information processing, information content, information format and information transfer standards across all functional areas (business, C3 and intelligence)
- **Sep 92** -- DISA's role expanded to adopting, developing, specifying, certifying and enforcing IT standards (to include weapon systems under DISA's purview)
- **Nov 92** -- SCC established as a sub-panel by MCEB per MCEB charter
- **FY 99** -- Congress assigns (Chapter 131, Title 10) DoD Chief Information Officer responsibility to "ensure that information technology and national security systems standards that will apply throughout the DoD are prescribed;..."

What is Information Technology (IT)?

**Public Law: Clinger-Cohen Act defines
Information Technology as:**

**“ Any equipment or interconnected system ... of equipment that is
used in automated**

- | | |
|----------------|----------------|
| - acquisition | - control |
| - storage | - switching |
| - manipulation | - interchange |
| - management | - transmission |
| - movement | - reception |

of data or information by the executive agency.”

What are National Security Systems?

Public Law: Clinger-Cohen Act defines National Security Systems (NSSs) as:

“Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

- involves intelligence activities;**
- involves cryptologic activities related to national security;**
- involves command and control of military forces;**
- involves equipment that is an integral part of a weapon or weapons system, or**
- is critical to the direct fulfillment of military or intelligence missions.”**

DoD IT Standards Directives & Policies

***DoD Instruction 4630.8 (18 Nov 92)* states that:**

- **CJCS will “assess compliance with U.S. standards and the Standardization Agreements (STANAGs)”**
- **DISA will “serve as the single point of contact for development of IT standards”**
- **DISA along with other DoD components must work together on IT standards development such that “...collaboration will be ensured by the DoD Standards Coordinating Committee (SCC). The SCC will ensure that standards prescribed for any new hardware or software are consistent with those of systems that they are to interoperate.”**

DoD IT Standards Directives & Policies (cont'd)

DoD Directive 5100.35 (10 Mar 98) states that:

- **The “MCEB shall consider those military communications-electronics matters, including National Security Systemsreferred to it by the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the DoD Chief Information Officer...”**
- **The MCEB Chair shall “Inform the DoD CIO of all MCEB-related matters, which may have an impact on the responsibilities of the CIO...”**

DoD IT Standards Directives & Policies (cont'd)

CJCS Instruction 6212.01B (8 May 00) states that:

Joint Staff, J6 Director will convene the Military Communications & Electronics Board (MCEB) to:

- “Act as the senior resolution body for issues related to NSS and ITS, standards, and interoperability issues.”
- Charter sub-panels and define their functions as needed, such as...
“The Standards Coordinating Committee (SCC, which) will resolve standards issues that arise in the MCEB process.”

Director, DISA will:

- “Exercise DISA’s role as executive agent for coordinating and integrating the DoD ITS standards activities.”
- “Manage the NSS and ITS Standards Program and administer the process to ensure that appropriate standards are available and used, including defining standards requirements and planning, prioritizing, and resourcing standards projects.”
- “Provide guidance, assistance, and information on appropriate use of standards, the applicability of standard to functional areas (e.g. networking), system domains (e.g. intelligence), and program phases (e.g. use of existing standards for imminent acquisitions and use of emerging standards for long-range program planning).”

DoD IT Standards Directives & Policies (cont'd)

SecDef Memo: “DoD Chief Information Officer Executive Board” (31 Mar 00) states that:

DoD CIO Executive Board provides...

“Management Oversight. Recommend, review and advise the DoD CIO on overall DoD IM policy, processes, procedures and standards.”

.....

DoD Directive 5137.1 (pending signature) states:

This ASD(C3I) charter directs that the DoD CIO shall...

“Ensure the development, coordination, implementation, and evaluation of IM and IT integrated architectures, management, programs, standards, processes, and interoperability of IT....”

DoD Chief Information Officer's (CIO) Role

Public Law-Title 10 states that:

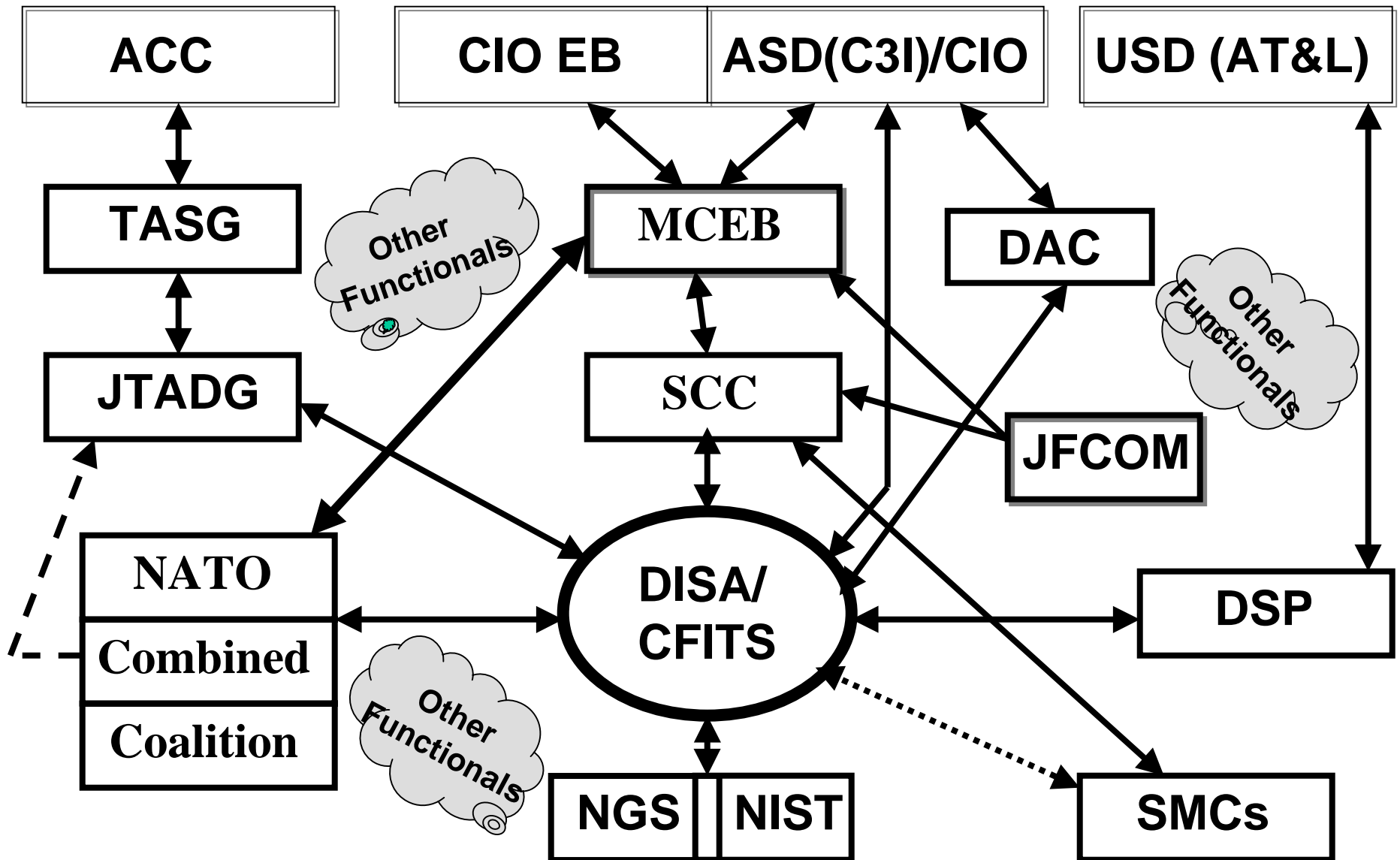
“The Chief Information Officer of the Department of Defense shall:

- Review and provide recommendations to the SECDEF on DoD budget requests for IT and NSS
- Ensure the interoperability of IT and NSS throughout DoD
- *Ensure that IT and NSS standards that will apply throughout the DoD are prescribed*
- Provide for the elimination of duplicate IT and NSS within and between the MILDEPs and Defense Agencies”

MCEB Pub 1: List of Current SCC Functions

- **Develop, review, comment and coordinate IT standards plans & policy**
- **Serve as focal point for CM of all IT standards programs**
- **Recommend approval/disapproval of IT standards and changes or deletions of IT standards to ensure compliance of DoD policies including those of DSP**
- **Develop guidance and direction for the Executive Agent CM activities related to USMTF and TADIL programs**
- **Review, for decision or referral, those issues or actions forwarded to it by the USMTF and TADIL CCBs**
- **Review, for decision or referral, those standards issues forwarded to it by the Data Systems Interoperability Panel**
- **Recommend IT standards project priorities to the DoD Executive Agent**
- **Recommend IT standards project initiation and propose appropriate project execution activities to the EA**
- **As directed by the MCEB, provide MCEB/DoD representatives to appropriate national and international technical panels/working groups and federal standards**
- **Charter subordinate IT standards bodies, as needed, to assist in accomplishing SCC function and responsibilities**
- **Review the IT Standards Management Plan every two years**
- **Coordinate or collaborate with other MCEB Panels on matters of mutual interest**
- **Meet with counterparts of the Combined Communications-Electronics Board (CCEB) on matters of mutual interest**

Standards Management “As Is” Process



Standards Management Committees: “As Is”

- **Information Transfer Standards Management Panel (IXMP)**
- **Satellite Communications (SATCOM) Interoperability & Standards Committee (SISC)**
- **Electronic Data Interchange (EDI) Standards Management Committee**
- **Joint Multi-TADIL Standards Working Group (JMSWG)**
- **DoD Multimedia/Optical Digital Technologies (ODT) Standards Working Group(M/ODT SWG)**
- **Symbology Standards Management Committee (SSMC)**
- **TADIL Configuration Control Board**
- **USMTF Standards Management Committee/Configuration Control Board**
- **Geospatial Standards Management Committee**
- **Imagery Standards Management Committee**

SMP Working Group Observations

A robust, easy to understand process for establishing, managing, integrating, and enforcing IT Standards and Architectures across DoD Agencies, Services, and CinCs is needed.

- *DoD IT standards management structure does not take into account the broader responsibilities of the DoD CIO:*
 - Clinger-Cohen Act assigns specific responsibilities to DoD CIO for ensuring IT standards are prescribed for all DoD
 - Overarching process for developing, coordinating, prescribing and enforcing IT and NSS standards and integrated architectures across all DoD is needed
 - Enforcement mechanisms are needed to ensure implementation, compliance with JTA, and conformance to all IT and NSS standards
- *The DoD IT environment has changed:*
 - Half-life for IT is <9 months... IT standards development is Industry/market driven predominating DoD's IT and NSS standards. Closer DoD/Industry liaison is needed
 - To participate better with Industry in establishing non-governmental standards (NGS), DoD must be more proactive, cohesive, and aggressive in coordinating its IT and NSS standards

SMP WG's Findings and *Recommendations*

1. Current DoD IT management structure fails to account for DoD CIO responsibilities mandated by Law.

- *SCC should focus on MILSTD coordination for NSS and IT systems, and should convene only when there are issues to be considered in order to conserve resources*
- *Expand oversight for IT standards and architectures to DoD CIO Executive Board*
- *DoD CIO/ASD(C3I) should charter an IPT to re-engineer and integrate DoD IT architecture and standardization processes for greater efficiency/ease of understanding, monitoring, and enforcement*
- *DoD IT EA (DISA) should ensure continuity in SCC leadership*
- *DoD IT EA (DISA) should review IT Standards Management Plan for relevance and value-added; update as appropriate*

SMP WG Findings and *Recommendations* (Cont'd)

2. Ineffective means to provide decision makers with visibility in IT standards issues. Process for comprehensive, top-down standards management direction is lacking. SCC is currently not sufficiently scoped or broad-based across the entire gamut of IT and NSS standardization areas of interest to all DoD.

- *DoD CIO Executive Board and MCEB should jointly confer and come to consensus on the role and mission of the SCC, its authority and oversight responsibilities, areas of concern, reporting chain, and enforcement mechanisms.*
- *IPT chartered by DoD CIO should develop guidance, direction, roles and missions, and operating procedures for use across all IT and NSS across DoD based on the IT Standards and Architecture integration requirements as they exist at this point in the evolution of technology and public law.*

SMP WG Findings and *Recommendations* (Cont'd)

3. Revised roles and missions across DoD, due to organizational restructuring and alignments (i.e., Unified Command Plan 99) have an impact on the “As Is”, current DoD IT standards management and architecture integration process.

Principal advocates for Interoperability (e.g. JFCOM) have a vested interest in IT standardization, but are not well-integrated into the standards management process which drives interoperability.

- DoD ACC, DoD CIO Executive Board and MCEB should jointly confer and clarify the how to integrate the roles and mission of Interoperability advocates in the IT and NSS Defense standardization processes, commencing with JFCOM as the primary Joint Force Integrator under UCP 99.*

SMP WG Findings and *Recommendations* (Cont'd)

4. Opportunity exists to streamline standards management process.

- *Consolidation of EB/EC, DAC, JTADG, TASG under single standards oversight body should be done to streamline and enhance the process*
- *Review MCEB Pubs 1 & 2 to update SCC roles, functions, and administrative procedures*
- *Review and consider restructuring SMCs*
 - *Document clear standards management process and reporting channels for SMCs*
 - *Draft charters for each SMC for approval by SCC*
 - *Require SMCs report issues/status of work to SCC within 90 days*
 - *Review and recommend revised MCEB charter to reflect changes*

Can Standards Management Process be Improved?

ABSOLUTELY!!

